

### *In the Claims*

The status of claims in the case is as follows:

1        1.    [Currently amended] Method for operating a first node  
2        in a network including at least one second node, comprising  
3        the steps of:

4            establishing at said first node a coincident endpoint  
5            for an outer connection and an inner connection with  
6            respect to at least one second node, said outer  
7            connection and said inner connection being IP security  
8            connections;

9            responsive to receiving ~~a-nested~~ an inbound nested  
10          packet from said second node on said outer connection,  
11          decapsulating said packet into a first packet and then  
12          performing source-in network address translation on  
13          said first packet; and

14          responsive to receiving ~~a-second~~ an outbound second  
15          packet at said inner connection, performing source-in  
16          network address translation on said second packet, and  
17          then encapsulating said second packet into a nested

18 packet for communication on said outer connection to  
19 said second node.

2. [Canceled]

1 3. [Currently amended] Method for managing connections  
2 within a communications system, comprising the steps of:

3 configuring an outer IP security connection;

4 communicating from a client to a gateway on said outer  
5 connection a request to configure a secure inner  
6 connection;

7 responsive to said request, initializing said gateway  
8 to receive a future nested communication, including  
9 obtaining a client address from a packet on said outer  
10 connection;

11 starting said inner connection;

12 responsive to starting said inner connection,  
13 propagating a network address translation rule from  
14 said outer connection to said inner connection.

1       4.   [Original]   The method of claim 3, further comprising  
2       the step of:

3           further responsive to starting said inner connection,  
4           encapsulating a packet outbound from said gateway first  
5           in said inner connection and then in said outer  
6           connection.

1       5.   [Original]   The method of claim 4, further comprising  
2       the steps of:

3           responsive to receiving a packet at said gateway,  
4           determining if said packet has a security header;

5           responsive to said packet having said security header,  
6           decapsulating said packet and saving any address  
7           translation rule included within said packet; and

8           applying said address translation rule to said packet  
9           and thereafter communicating said packet from said  
10          gateway to said client.

1       6.   [Original]   The method of claim 5, further comprising  
2       the steps of:

3           iteratively executing said decapsulating step until a  
4           resulting decapsulated packet no longer contains a  
5           security header.

1       7.   [Currently amended]   Method for enabling a local  
2       gateway to handle dynamically assigned IP addresses from  
3       remote clients, comprising the steps of:

4           assigning said IP address to a remote client;

5           automatically maintaining between said remote client  
6           and said gateway nested IP security connections with  
7           local coincident endpoints.

1       8.   [Original]   The method of claim 7, wherein said nested  
2       connections comprise an inner connection and an outer  
3       connection.

1       9.   [Currently amended]   The method of claim 8, further  
2       comprising the steps of:

3 responsive to receiving ~~a nested~~ an inbound nested  
4 packet from said client on said outer connection,  
5 decapsulating said packet into a first packet and then  
6 performing source-in network address translation on  
7 said first packet; and

8 responsive to receiving ~~a second~~ an outbound second  
9 packet at said inner connection, performing source-in  
10 network address translation on said second packet, and  
11 then encapsulating said second packet into a nested  
12 packet for communication on said outer connection to  
13 client.

1 10. [Currently amended] System for operating a first node  
2 in a network including at least one second node, comprising:

3 an inner IP security connection;

4 an outer IP security connection;

5 a local coincident endpoint for said outer connection  
6 and said inner connection at said first node with  
7 respect to at least one second node;

8           said first node being responsive to receiving ~~a nested~~  
9           an inbound nested packet from said second node on said  
10          outer connection for decapsulating said packet into a  
11          first packet and then performing source-in network  
12          address translation on said first packet; and

13          said first node being further responsive to receiving ~~a~~  
14          ~~second~~ an outbound second packet at said inner  
15          connection for performing source-in network address  
16          translation on said second packet, and then  
17          encapsulating said second packet into a nested packet  
18          for communication on said outer connection to said  
19          second node.

1       11. [Currently amended] Method for extending virtual  
2       private network (VPN) network address translation (NAT) to  
3       include support for nested connections with coincident  
4       endpoints, without requiring any special configuration for  
5       the inner (nested) VPN connection, with respect to VPN NAT,  
6       comprising the steps of:

7           configuring an outer IP security connection with a VPN  
8           NAT rule;

9 communicating from a client to a gateway on said outer  
10 connection a dynamically generated security association  
11 request packet to configure a secure inner connection;  
  
12 responsive to said request, initializing said gateway  
13 to receive a future nested communication, including  
14 obtaining a client address from said request packet on  
15 said outer connection;  
  
16 starting said inner connection;  
  
17 responsive to starting said inner connection,  
18 propagating said VPN NAT rule from said outer  
19 connection to said inner connection.

1 12. [Original] The method of claim 11, further comprising  
2 the step of:

3 further responsive to starting said inner connection,  
4 encapsulating a packet outbound from said gateway first  
5 in said inner connection and then in said outer  
6 connection.

1       13. [Original] The method of claim 12, further comprising  
2       the steps of:

3               responsive to receiving a packet at said gateway,  
4               determining if said packet has a security header;

5               responsive to said packet having said security header,  
6               decapsulating said packet and saving any VPN NAT rule  
7               included within said packet; and

8               applying said NAT rule to said packet and thereafter  
9               communicating said packet from said gateway to said  
10              client.

1       14. [Original] The method of claim 13, further comprising  
2       the step of:

3               iteratively executing said decapsulating step until a  
4               resulting decapsulated packet no longer contains a  
5               security header.

1       15. [Canceled]



2     16. [Currently amended] System for extending virtual  
3     private network (VPN) network address translation (NAT) to  
4     include support for nested connections with coincident  
5     endpoints, without requiring any special configuration for  
6     the inner (nested) VPN connection, with respect to VPN NAT,  
7     comprising:

8             a gateway;

9             a client;

10            an inner IP security connection for connecting said  
11            gateway and said client;

12            an outer IP security connection for connecting said  
13            gateway and said client;

14            said outer connection being configured by said client  
15            with a VPN NAT rule;

16            said outer connection for communicating from said  
17            client to said gateway a dynamically generated security  
18            association request packet to configure said inner  
19            connection;

20        said gateway further responsive to said request for  
21        initializing said gateway to receive a future nested  
22        communication, including obtaining a client address  
23        from said request packet on said outer connection;

24        said gateway further responsive to starting said inner  
25        connection for propagating said VPN NAT rule from said  
26        outer connection to said inner connection.

1        17.    [Currently amended] A program storage device readable  
2        by a machine, tangibly embodying a program of instructions  
3        executable by a machine to perform method steps for  
4        operating a first node in a network including at least one  
5        second node, said method steps comprising:

6        establishing at said first node a coincident endpoint  
7        for an outer connection and an inner connection with  
8        respect to at least one second node, said outer  
9        connection and said inner connection being IP security  
10       connections;

11       responsive to receiving ~~a-nested~~ an inbound nested  
12       packet from said second node on said outer connection,  
13       decapsulating said packet into a first packet and then

14 performing source-in network address translation on  
15 said first packet; and

16 responsive to receiving ~~a second~~ an outbound second  
17 packet at said inner connection, performing source-in  
18 network address translation on said second packet, and  
19 then encapsulating said second packet into a nested  
20 packet for communication on said outer connection to  
21 said second node.

1 18. [Currently amended] A computer program product or  
2 computer program element for operating a first node in a  
3 network including at least one second node according to the  
4 steps of:

5 establishing at said first node a coincident endpoint  
6 for an outer connection and an inner connection with  
7 respect to at least one second node, said outer  
8 connection and said inner connection being IP security  
9 connections;

10 responsive to receiving ~~a nested~~ an inbound nested  
11 packet from said second node on said outer connection,  
12 decapsulating said packet into a first packet and then

13 performing source-in network address translation on  
14 said first packet; and

15 responsive to receiving ~~a second~~ an outbound second  
16 packet at said inner connection, performing source-in  
17 network address translation on said second packet, and  
18 then encapsulating said second packet into a nested  
19 packet for communication on said outer connection to  
20 said second node.

1 19. [Currently amended] A program storage device readable  
2 by a machine, tangibly embodying a program of instructions  
3 executable by a machine to perform method steps for managing  
4 connections within a communications system, said method  
5 steps comprising:

6 configuring an outer IP security connection;

7 communicating from a client to a gateway on said outer  
8 connection a request to configure a secure inner  
9 connection;

10 responsive to said request, initializing said gateway  
11 to receive a future nested communication, including

12           obtaining a client address from a packet on said outer  
13           connection;

14           starting said inner connection;

15           responsive to starting said inner connection,  
16           propagating a network address translation rule from  
17           said outer connection to said inner connection.

1       20. [Original] The storage device of claim 19, said method  
2       steps further comprising the step of:

3           further responsive to starting said inner connection,  
4           encapsulating a packet outbound from said gateway first  
5           in said inner connection and then in said outer  
6           connection.

1       21. [Original] The storage device of claim 20, said method  
2       steps further comprising the steps of:

3           responsive to receiving a packet at said gateway,  
4           determining if said packet has a security header;

5           responsive to said packet having said security header,

6           decapsulating said packet and saving any address  
7           translation rule included within said packet; and  
  
8           applying said address translation rule to said packet  
9           and thereafter communicating said packet from said  
10          gateway to said client.

1       22. [Original] The storage device of 21, said method steps  
2       further comprising the steps of:

3           iteratively executing said decapsulating step until a  
4           resulting decapsulated packet no longer contains a  
5           security header.